New Hardware Security Solution Roll Out:
the New Secure OTP Solution and Multi-Dimensional Root of Trusts Delivery to SoC Chips

eMemory

ABSTRACT

With the advent of various IoT applications, wireless connected IoT devices open up new possibilities to hackers and new threats to personal privacy and property. Autotronics, such as ADAS and Self-Driving, is regarded as one of next driving force for semiconductor industry and will rely on the hardware security protection for the human safety. Moreover, with big progress of leading high-performance-computing FinFET process (HPC/HPC+) delivered by tsmc, the emerging Machine Learning (ML) and AI technologies will advance at incredible acceleration speed. However, how to secure the proprietary ML/AI's model & algorithm or intellectual property safely will be the next serious security topic that needs lots of focus.

eMemory, as the leading company providing logic-NVM technologies, has long-term partnership with TSMC since 2002. eMemory's Logic NVM IP can provide essential and critical hardware security key and configuration for authentication and authorization. With high quality that meets TSMC 9000 IP compliance, eMemory logic NVM IPs have been successfully qualified and mass production at tsmc mature, more than Moore, and leading-edge FinFET technology nodes.

To provide comprehensive security protections to tsmc's customers, the eMemory's security solutions have been rolled out at least three generations by strong R&D's bandwidth and innovative ideas. The 1st GEN security IP (verified in tsmc 90EF, 40/55 LP/ULP, 28LP/HPC/HPC+, 16FFC etc..), similar to other anti-fuse based OTP solutions, relies on the intrinsic and invisible memory cell characteristics. The secret data stored in raw OTP memory array still needs many security protection circuits designed from SoC chips (namely, by IC design house) to prevent the secret leak.

Firstly, this presentation will address the eMemory's 2nd GEN solution, differentiating from other OTP IPs, was built-in critical security features (multi-power detections, anti-tampering, fault-injection detection and side-channel-attack mitigation etc.), offering tsmc's customers the comprehensive security protections against security attacks. This security IP was verified/qualified in tsmc 28nm HPC+ (1.8V) & 10nm FinFET and successfully pass the security certification by international Condition Access (CA) company. It reduces the security design barriers and benefits most IoT customers with full protections on secret data.

With persistence, eMemory recently rolled out new security solution (3rd GEN) and set a new benchmark on secure OTP IP solution. This presentation will address the new hardware Random Number Seeds (RNS) seamlessly integrated in eMemory's OTP solution which was verified in tsmc 55ULP, enabling each SoC chips embedded eMemory's OTP IP with its unique encryption approaches. By leveraging the eMemory's truly and cryptographically RNS technique, the highest secure OTP solution and multi-dimensional root of trusts will be able to deliver to tsmc's customers with robust mass production, resist to malicious security invasions and 150^{o}C (or above) stringent and harsh environments.

New Hardware Security Solution Roll Out:
the New Secure OTP Solution and Multi-Dimensional Root of Trusts Delivery to SoC Chips

Hsin-Ming Chen

eMemory Technology Inc.

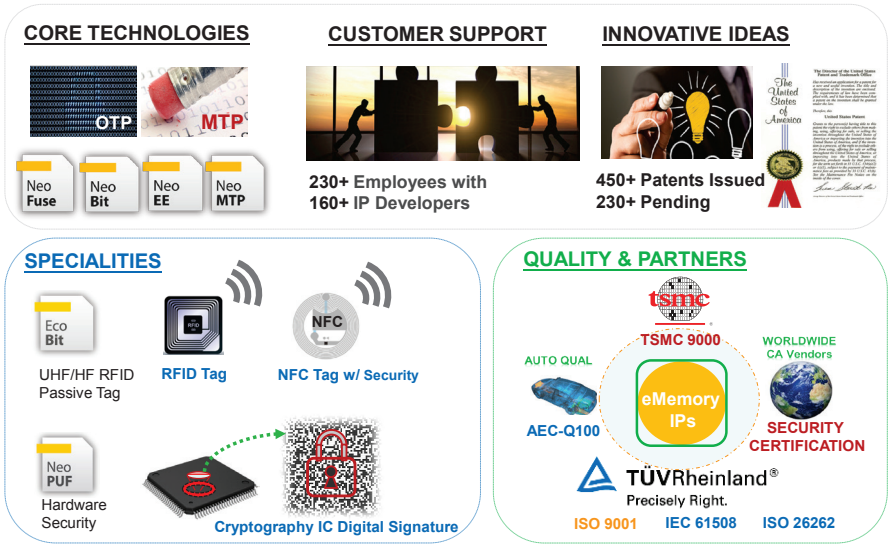
Sep. 2017

IPR Notice

Outlines

- About eMemory
- GEN1- Invisible and Reliable NeoFuse Security IP
- GEN2- Comprehensive Security Features in NeoFuse IP
- GEN3- Roll out new generation NeoFuse IP with True Random Number Seed as Security Root of Trust
- Summary

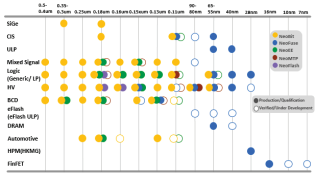
Corporate Overview



Corporate Overview

WIDE AVAILABILITIES

Production Map



0.5um~7nm; 350+ process nodes

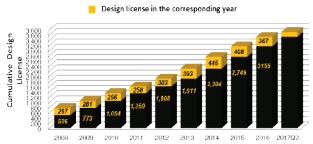
WIDE APPLICATIONS

30+ IC Types; 100+ Applications

WORLDWIDE CUSTOMERS

1300+ Customers;1240+ IPs

DESIGN WINS



>3700 NTOs

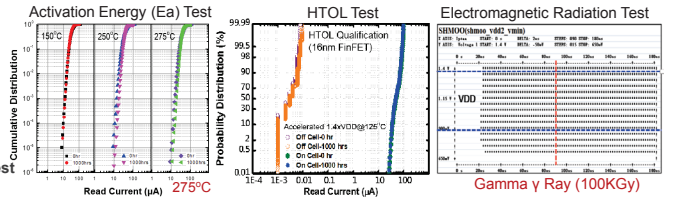
AWARDS

TSMC Best IP Partner

NeoFuse Security IP (GEN I)

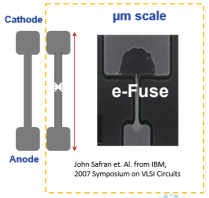
Rigorousness

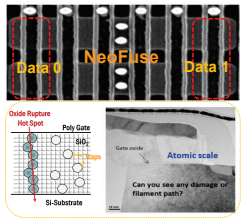
- Retentivity Test
- Long Term Read Lifetime Test
- Radiation Hardness Test



Invisibility required for Security

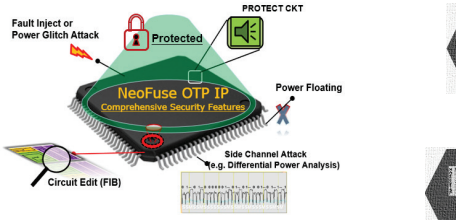
- Against Security Vulnerability
- Tiny Filament (Atomic Scale) formed in Programmed cells
- Resistance to Invasive Attacks





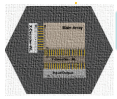
eNVM Bit Streams Expansion

NeoFuse Security IP (GEN II)

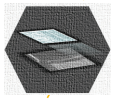


Invasive attack	Semi-Invasive attack	Non-Invasive attack
Reverse Engineering	Optical Fault Injection	Timing Analysis
Micro-probing	Backside Image	Power Analysis
Circuit Edit	UV Erase	Power Glitching
VC Inspection	Electromagnetic Attack	Data Tampering

- **Bit level Lock**
  - Built-in charge pump
  - Bit program lock to Auto Stop illegal data modification



- **Address Scrambling**
  - 3 Levels Address Scrambling
  - Make a confusion to adversaries



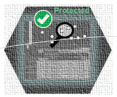
- **Metal Shielding**
  - Inactive CKT functionality when FIB circuit edit on sensitive circuit
  - Warning SoC chip when Top Metal layer cracking

- **Security Oriented Layout Design**
  - Layout review in detail by international Security CA partner

Neo Fuse GEN2

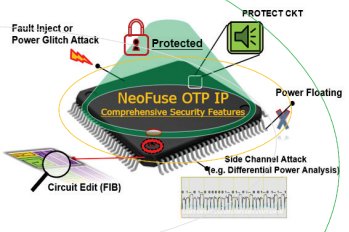
NeoFuse Security IP (GEN II)

Security Certification



Against Voltage Contrast

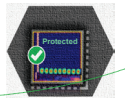
Resistance to DPA (Differential Power Analysis)



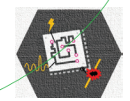
Protection on Output Data Fault Injection

Secure Repair

Alarm System to SoC Chip



Safe to Photonic Emission Attack



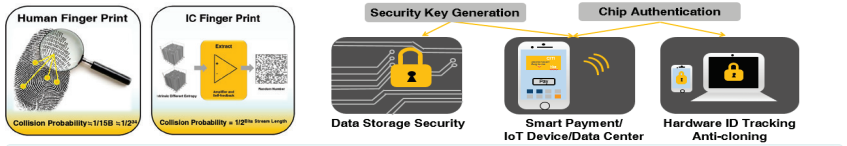
Multi-Level Power Detections

Neo Fuse GEN2

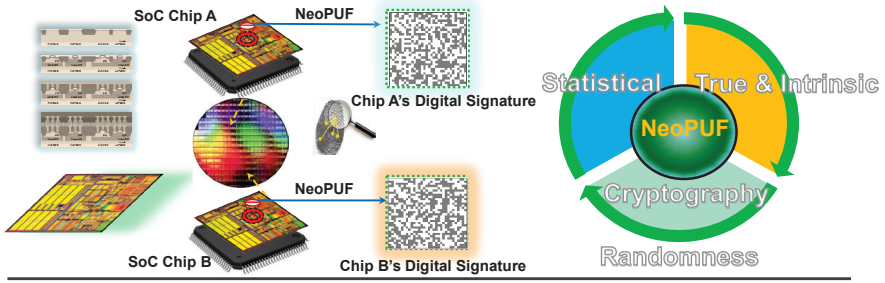
New OTP Security Benchmark Roll out

Build Unique IC Fingerprint & Unclonable ID inside every SoC Chips

Human Finger Print › IC Chip Finger Print › Security Keys Generation and Secure Chip Authentication



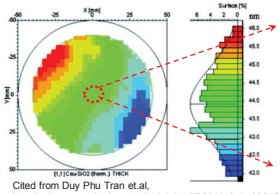
1 Entropy Source: Manufacturing Variations 2 Extraction by NeoPUF 3 NeoPUF as Random Number Seed with



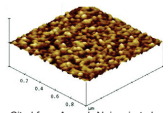
NeoPUF Technology Features

UNPREDICTABILITY | UNIQUENESS | ROBUSTNESS

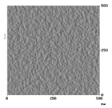
- **Natural Born Random Number Seed**
  - Entropy source from Physical Process Variations
  - Two identical PUF cells Competing on physical behaviors
  - Unpredictable Randomness



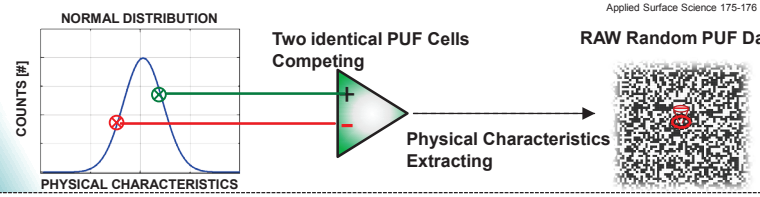
Cited from Duy Phu Tran et.al, http://pubs.rsc.org/en/content/articlehtml/2014/tc/c4tc00046c



Cited from Aneesh Nainani et.al, Journal of Applied Physics (Jun 2011)

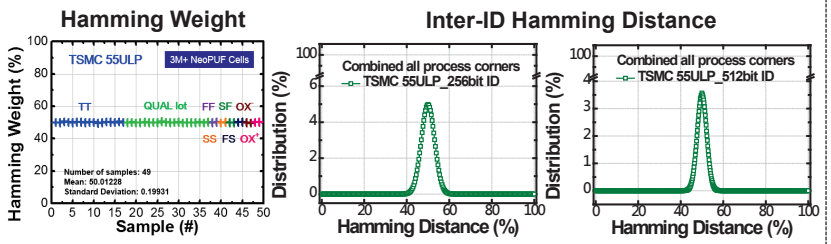


Cited from P.Mur et.al, Applied Surface Science 175-176 (2001)



NeoPUF Technology Features

UNPREDICTABILITY | UNIQUENESS | ROBUSTNESS



- **Hamming Weight test**
  - Hamming Weight (HW): Defined as % of "1" bits in PUF Bit String
  - "Intrinsic" and "Un-biased" Randomness
  - No Post Processing is needed to balance the numbers for data "0" and "1"
- **Inter-ID Hamming Distance test**
  - Peak at 50% Distance
  - Irrelative to process corners
  - Irrelative to Bit Strings (256 bits or 512bits)
  - Randomness & Uniqueness demonstrated

NeoPUF Technology Features

UNPREDICTABILITY | UNIQUENESS | ROBUSTNESS

- **NIST 800-22 Statistical Test**
  - TSMC 55ULP corners wafers (TT/FF/SS/FS/SF/OX+/OX-)
  - PASS all items (15+1 items & its sub-test items)

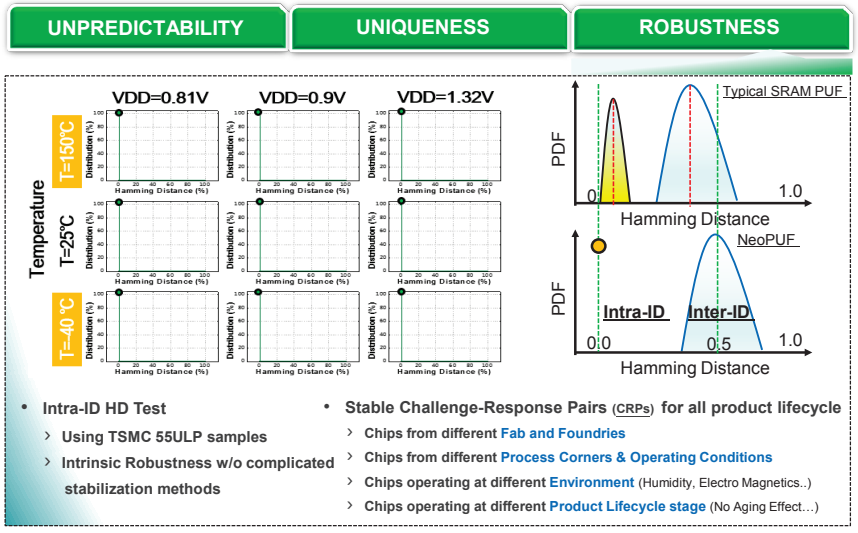
3M+ NeoPUF Cells

#	Statistical Test	Recommended n	Input Size		Sub-Test #	Decision Rule					Randomness Judgement
		Length of bit string	n	bit stream(s)		Min. P-Value	Proportion		Uniformity		PASS/FAIL
						P-Value > 0.01	mini	P/F	P-value of P-value > 0.0001	P/F	
1	Frequency	n>100	40000	75	1	-	73/75	PASS	0.238562	PASS	PASS
2	Block Frequence (m=128)	n>100	40000	75	1	-	73/75	PASS	0.72554	PASS	PASS
3	Cumulative sums - Forward	n>100	40000	75	1	-	74/75	PASS	0.519916	PASS	PASS
4	Cumulative sums - Reversed	n>100	40000	75	1	-	74/75	PASS	0.72554	PASS	PASS
5	Runs	n>100	40000	75	1	-	73/75	PASS	0.362174	PASS	PASS
6	Longest runs of ones	n>128	40000	75	1	-	73/75	PASS	0.295803	PASS	PASS
7	Binary Matrix Rank	n>38912	40000	75	1	-	73/75	PASS	0.808725	PASS	PASS
8	Spectral DFT	n>1000	40000	75	1	-	73/75	PASS	0.937294	PASS	PASS
9	Non-overlapping Templates (m=9)	n>8m-8	40000	75	148	-	71/75	PASS	0.00058	PASS	PASS
10	Overlapping Templates (m=9)	n>1E6	40000	75	1	-	73/75	PASS	0.036868	PASS	PASS
11	Serial (m=16, ∇Psi2)	m< (log2 n)-2	40000	75	2	-	73/75	PASS	0.127486	PASS	PASS
12	Approximate Entropy (m=10)	m< (log2 n)-5	40000	75	1	-	73/75	PASS	0.339544	PASS	PASS
13	Universal	n>387840	1000000	3	1	0.341243	3/3	PASS	-	-	PASS
14	Linear complexity (M=500)	n>1E6	1000000	3	1	0.652199	3/3	PASS	-	-	PASS
15	Random Excursions	n>1E6	1000000	3	8	0.145246	3/3	PASS	-	-	PASS
16	Random Excursions Variant	n>1E6	1000000	3	18	0.036142	3/3	PASS	-	-	PASS

- **AIS-31 Statistical Test**
  - TSMC 55ULP, including corners (TT/FF/SS/FS/SF/OX+/OX-)
  - PASS all items (P1+P2 and its sub-test items)

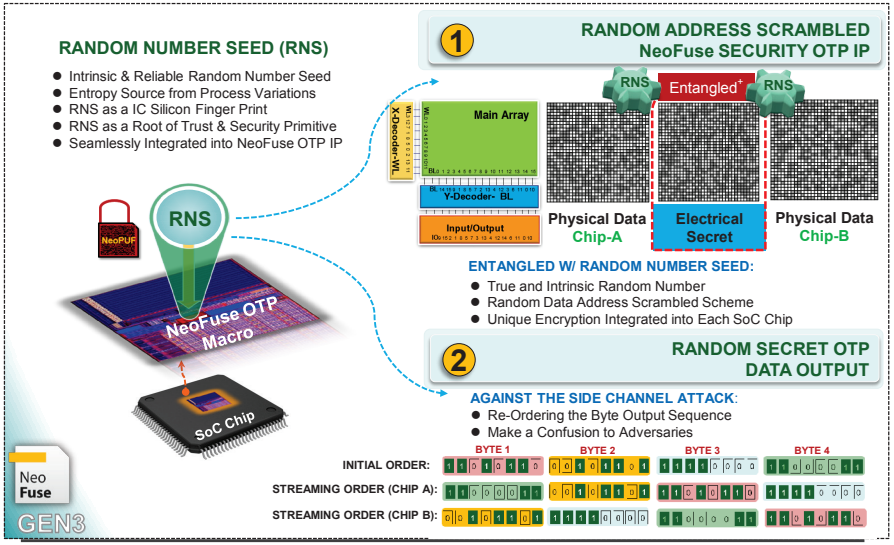
	AIS-31 Statistical Tests	Minimum Length of bit string	Sub-Test #	Test Result		PASS/FAIL
P1	T0: Disjointness test	$2^{16} * 48$	1	Test T0 bestanden	Durchlauf erfolgreich beendet PASS (Complete and Successful)	PASS
	T1: Monobit test	257 * 20000	257	Test T1 bestanden		PASS
	T2: Poker test	257 * 20000	257	Test T2 bestanden		PASS
	T3: Runs test	257 * 20000	257	Test T3 bestanden	Durchlauf erfolgreich beendet PASS (Complete and Successful)	PASS
	T4: Long run test	257 * 20000	257	Test T4 bestanden		PASS
	T5: Auto-correlation test	257 * 20000	257	Test T5 bestanden		PASS
P2	T6a: Uniform distribution test	100000	1	Testprozedur T6a bestanden	Durchlauf erfolgreich beendet PASS (Complete and Successful)	PASS
	T6b: Uniform distribution test	100000	1	Testprozedur T6b bestanden		PASS
	T7a: Homogeneity test	100000	2	Testprozedur T7a bestanden		PASS
	T7b: Homogeneity test	100000	4	Testprozedur T7b bestanden		PASS
	T8: Entropy estimation test	7200000	1	Test T8 bestanden		PASS

NeoPUF Technology Features

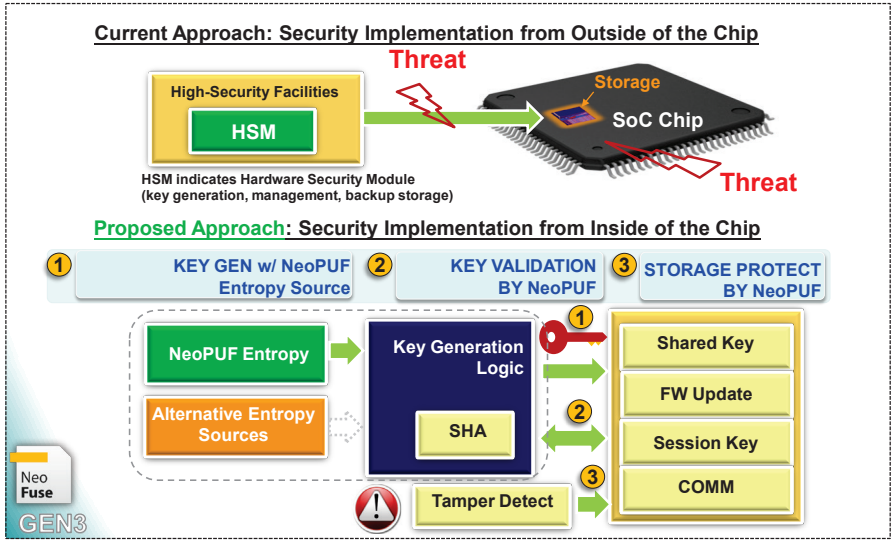


- Intra-ID HD Test
  - Using TSMC 55ULP samples
  - Intrinsic Robustness w/o complicated stabilization methods
- Stable Challenge-Response Pairs (CRPs) for all product lifecycle
  - Chips from different Fab and Foundries
  - Chips from different Process Corners & Operating Conditions
  - Chips operating at different Environment (Humidity, Electro Magnetics..)
  - Chips operating at different Product Lifecycle stage (No Aging Effect…)

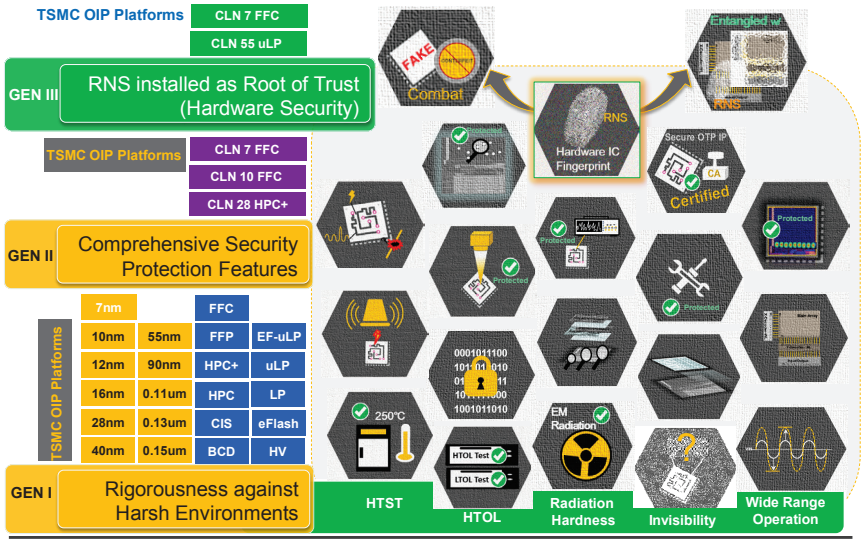
NeoFuse Security IP (GEN III)



NeoFuse Security IP (GEN III)



NeoFuse Security IPs (in TSMC OIP Platforms)



Summary

- **1st GEN NeoFuse IP, as the invisible memory characteristics, verified in most TSMC OIP platforms and meets the TSMC 9000 quality compliance for high yield, high reliability and high security applications**
- **Comprehensive security features have been successfully built in the 2nd GEN NeoFuse security IP by continuous innovation and mutual collaboration with international security partners.**
- **With 3rd GEN NeoFuse security IP rolling out,**
  - **Hardware-base security was established**
  - **Unpredictable, unique and robust Random Number Seed enabled by NeoPUF technology has been successfully installed into NeoFuse security IP**
  - **Multi-dimensional Root of Trusts can be delivered to SoC chips**

Embedded Wisely, Embedded Widely